IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

HARRIS CORPORATION,

Plaintiff,

v.

HUAWEI DEVICE USA, INC.,
HUAWEI DEVICE CO., LTD.,
HUAWEI TECHNOLOGIES USA INC.,
HUAWEI TECHNOLOGIES CO. LTD., AND
HUAWEI DEVICE (SHENZHEN) CO., LTD.

Defendants.

No. 2:18-cv-439-JRG (LEAD CASE)

Jury Trial Demanded

DECLARATION OF ANDREW T. RADSCH
IN SUPPORT OF HUAWEI'S RESPONSE IN OPPOSITION TO
HARRIS'S MOTION TO AMEND P.R. 3-1 INFRINGEMENT CONTENTIONS

I, Andrew Radsch, declare as follows:

1. I am a partner at the law firm of Ropes & Gray LLP, counsel for defendants ("Huawei") in this action. I submit this declaration in support of Huawei's Response in Opposition to Harris's Motion to Amend P.R. 3-1 Infringement Contentions.

2. Harris's asserted U.S. Patent No. 7,440,572 ("'572 patent"), filed on January 16, 2001 (Dkt. 13-7 at cover), states in the "Background of the Invention" section that WEP encryption was a known solution: "Security is addressed in the 802.11 standard as an option and may be accomplished by an encryption technique known as the ***Wired Equivalent Privacy (WEP) algorithm.***" *Id.* Col. 1, lns. 46-48 (emphasis added).

3. Harris's '678 and '690 patents were filed on August 12, 2002. Dkts. 13-5 and 13-6 at cover. In its amended contentions for those patents, Harris cites to WEP technology as a basis for its contention that accused phones, tablets, and laptops meet the policing station and intrusion detection limitations. For example, in its disclosure for the "policing station" limitation of claim 12 of the '678 patent, Harris states the following (highlighting added):

> Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also implement intrusion detection according to the claim. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

4. With respect to its "mobile hotspot" theory, the entirety of Harris's disclosure for the limitation "monitoring transmissions among said plurality of stations to detect failed attempts to authenticate MAC addresses" ('678 patent, cl. 12), is:

> On information and belief Huawei consumer devices, including laptops, phones and tablets also can monitor for failed MAC address authentications, including when configured as a mobile hotspot.

5. Similarly, for the limitation "generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address" ('678 patent, cl. 12), the entirety of Harris's disclosure for its "mobile hotspot" theory is:

> On information and belief Huawei consumer devices, including laptops, phones and tablets also can generate an intrusion alert based on monitoring for failed MAC address authentications, including when configured as a mobile hotspot.

6. For Harris's "WiFi threat detection" theory, Harris utilizes similarly conclusory language, and for each "policing station" and related intrusion detection limitation of the asserted claims, Harris quotes identical content from a single whitepaper. For example, for the "monitoring" limitation referenced in paragraph 5 above, Harris's disclosure is:

> Huawei consumer devices, including laptops, phones and tablets implementing the security features of Huawei's EMUI operating system, including its "Wi-Fi threat detection" functionality, also monitor for failed MAC address authentications. *See, e.g.*, EMUI 8.0 Security Technical White Paper, available at https://consumer-img.huawei.com/content/dam/huawei-cbg-site/en/mkt/legal/privacy-policy/EMUI%208.0%20Security%20Technology%20White%20Paper.pdf, at 15 ("Wi-Fi connection can be authenticated using various methods, such as WEP, WPA/WPA2 PSK, 802.1x EAP, WPS, and WAP" and "EMUI provides Wi-Fi threat detection engine on access points. It detects the Wi-Fi to be connected. Once security risks are detected, it will notify users so that they can take measures to ensure connection security.").

7. Harris's original Contentions accuse the following **six** phone models: Mate SE, Porsche Design Huawei Mate 10, Mate 10 Pro, Mate 9, Ascend XT², and Elate.

8. Harris's amended contentions seek to add the following **twenty-three** phone models: Porsche Design Huawei Mate RS, Porsche Design Huawei Mate 20 RS, Mate 20, Mate 20 Lite, Mate 20 Pro, Mate 20 X, P20, P20 Lite, P20 Pro, P30, P30 Lite, P30 Pro, Honor 7X, Honor 8, Honor 8A, Honor 8X, Honor 10, Honor 10 lite, Y7, Y9, nova 3, nova 4, P Smart.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on August 25, 2019. /s/ Andrew T. Radsch